Restricted Content

Critical Risk Management

A Good Practice Guide **2027**

This guide helps *Persons Conducting a Business or Undertaking* (PCBUs) prevent serious harm and meet obligations under the *Health and Safety at Work Act 2015.*

DRAFT

Work can cause death, life-changing injury, or serious illness when the controls relied on to prevent harm are missing, weakened, or ineffective.

This guide helps PCBUs identify critical risks, establish the controls that matter most, and check that they work in practice. It sets out principles of good Critical Risk Management; the supporting implementation toolkits provide detailed methods and tools.

Acknowledgements

This guide draws on international good practice, standards, and consultation with New Zealand PCBUs at different stages of Critical Risk Management.

Particular appreciation is given to the members of the health and safety community who provided input and advice, and the project team for their dedication and expertise, namely:

- Rob Mair – Project Group Chair
- Wendi Bains – Deputy Project Group Member
- Chris Jones – Lead Author
- Tracy Evans-Tracy – Consultation Lead
- Will Eastgate – Project Group Member
- Yolanda Oosthuizen – Project Group Member
- Elaine Toal – Project Group Member
- Louis Buckingham – Project Group Member
- Guy Smith – Project Group Member

Restricted Content

Contents

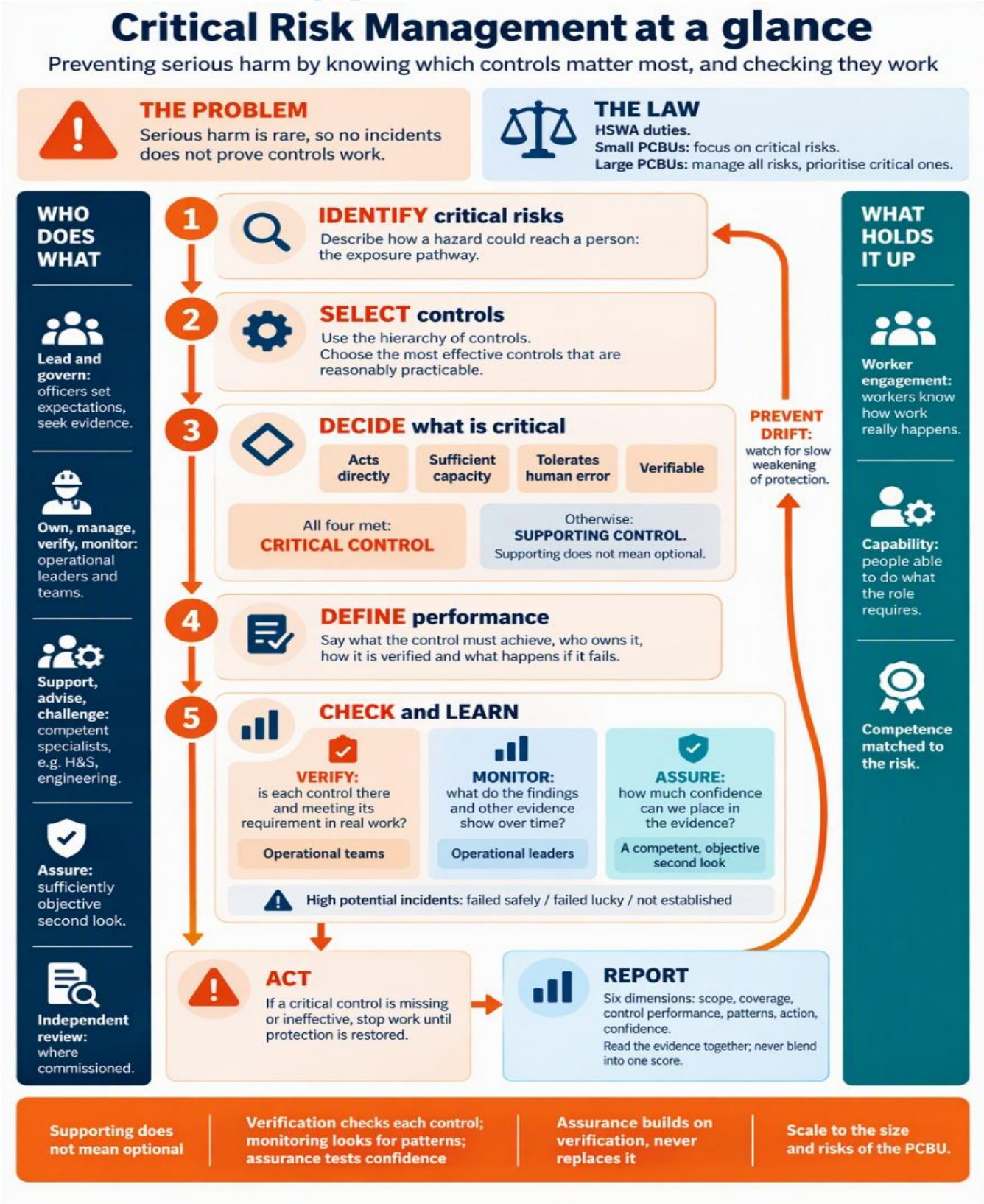
Acknowledgements 1
1. The Problem 5
2. Legal Context 6
3. Overview 7
4. Accountability, Leadership, and Assurance 10
Who manages critical risks – and who supports them 10
Worker engagement and participation 12
Critical Risk Governance 12
Critical Risk Leadership 13
5. Identifying and Assessing Critical Risks 14
Identify critical risks 14
Describe exposure pathways 14
Assess control needs 15
Risks that are not critical 15
6. Selecting and defining critical controls 16
Use the hierarchy of controls 16
Assess whether the proposed controls will be effective 16
Determine what is reasonably practicable and justify control selection 16
Identify the critical controls 17
Examples of critical controls and supporting measures 19
Define control performance and ownership 20
Embed critical risks and controls in systems and decisions 20
7. Critical control verification, monitoring and assurance 22
Why verification matters and what it must establish 22
Verification responsibility 23
Verification: checking that critical controls work 24
Monitoring: what does the evidence show over time? 24
Assurance: a competent second look at the evidence 24
Interpret evidence from high potential incidents 25
Act on findings 26
8. Capability 27
9. Measurement and reporting 28
Measuring and reporting what matters 28

Interpret results in context 32
Use reporting to support decisions and action 32
10. Preventing drift in critical risk management 33
Appendix A: Examples of critical risks 34
Appendix B: Illustrative critical controls for defined exposure pathways 36
Appendix C: Technical foundations and further guidance 38

Restricted Content

The Guide at a Glance

This page summarises how the key concepts in the guide fit together: how critical risks and controls are identified and defined, how verification, monitoring and assurance work together, who does what, and what holds the system up. Use it as a map to the sections that follow.



Restricted Content

1. The Problem

Despite sustained effort across New Zealand and internationally, work-related fatalities, serious injuries, and serious illnesses remain a significant challenge.

Serious-harm events can be infrequent, and serious illness can develop over years from repeated or prolonged exposure with no single event to prompt attention. An absence of incidents involving risks that can cause serious harm may lead PCBUs to believe that effective controls are in place and working – until an incident occurs or a disease emerges and it is discovered that a relied-upon control was absent, degraded, bypassed, or ineffective.

Critical Risk Management therefore focuses PCBUs' efforts on risks capable of causing death, serious injury or illness, a notifiable incident or an occupational disease. It guides PCBUs to understand how harm could occur, establish the controls most relied upon to prevent or mitigate it, verify their performance, and act on findings.

Critical Risk Management sits within broader health and safety management and does not replace other applicable duties. Section 2 explains the different scopes of duty that apply to small and large PCBUs.

Restricted Content

2. Legal Context

This guide reflects the *Health and Safety at Work Act 2015* (HSWA), as amended by the Health and Safety at Work Amendment Act 2026. The amended duties and critical-risk framework took effect on 1 April 2027.

HSWA requires PCBUs to protect workers and others affected by their work so far as is reasonably practicable, within the applicable scope of their duties.

A core objective of HSWA is the prevention of work-related death, serious injury, and serious illness. Effective Critical Risk Management supports this objective by focusing attention on critical risks and the controls most relied upon to prevent serious harm.

PCBUs should use the statutory definitions and current regulator guidance to determine which duties apply to them:

- **Small PCBUs:** main HSWA risk-management duties generally apply only to critical risks.
- **Large PCBUs:** must manage all risks but prioritise critical risks through greater attention and share of risk-management resources, and more frequent monitoring, review, and revision of controls.

For the rules on worker numbers, including contractors and fluctuating workforces, use WorkSafe's *Am I a small or large PCBU?* Read it alongside *Managing critical risks for small PCBUs* or *Prioritising critical risks for large PCBUs*, as applicable.

HSWA defines critical risks through two routes:

1. association with a Schedule 1A hazard; or
2. association with another hazard where occurrence of the risk is likely to result in death, notifiable injury or illness, a notifiable incident, or an occupational disease listed in Schedule 2 of the Accident Compensation Act 2001. This concerns the likely consequence if the risk occurs, not simply how often an event is expected.

Section 5 explains how PCBUs should identify critical risks arising from their work and operating context.

Note: This guide is not legal advice. PCBUs should apply it alongside HSWA, relevant regulations and current regulator guidance, including applicable Approved Codes of Practice. It supports compliance and the prevention of serious harm; it does not replace those requirements.

Restricted Content

3. Overview

This guide sets out principles of good practice for managing critical risks and supporting compliance with HSWA. It covers the identification of critical risks, selection of effective critical controls, verification of control performance, and prevention of serious harm. Appendix C identifies the technical foundations and further guidance that inform this guide.

Effective Critical Risk Management helps a PCBU meet its duties through a continuous improvement cycle (see below) involving: identifying and prioritising critical risks; establishing and maintaining effective critical controls; verifying their performance; monitoring what the evidence shows across the work and over time; and using findings to strengthen protection. Together, this provides better information for decisions about work, risks, controls, resources, and improvement, and helps officers of the PCBU exercise due diligence and assess whether the PCBU is meeting its obligations.

Psychosocial risks may also meet the legal definition of a critical risk, but detailed psychosocial risk assessment and control is outside the scope of this guide. PCBUs should use appropriate specialist psychosocial-risk guidance, such as WorkSafe's Managing psychosocial risks at work. This scope decision does not change a risk's classification and does not remove any legal duty to identify and manage psychosocial risks.



The table below defines key concepts and their main qualifications.

Concept	Meaning	Why it matters / key qualification
Critical risks	Risks associated with Schedule 1A hazards, or other hazards where occurrence of the	Focus attention on the risks with the most serious

Concept	Meaning	Why it matters / key qualification
	risk is likely to result in death, notifiable injury or illness, a notifiable incident or a listed occupational disease.	consequences, such as a person being struck by mobile plant or developing permanent hearing loss from long-term noise exposure.
Critical controls	In this guide, a critical control is one that meets all four of the following criteria: 1. acts directly on the hazard or exposure pathway; 2. has sufficient capacity to prevent the defined exposure from causing serious harm; 3. once established, is designed to keep protecting people even if they make mistakes, forget something or lose attention during the work; and 4. has performance that can be defined and objectively verified.	Focuses resources and verification on the controls most capable of preventing serious harm, rather than treating all controls as the same. All four criteria must be met. Section 6 explains the criteria and their limits.
Supporting controls	Controls that help establish, operate, maintain or check protection, or that contribute to protection but do not meet all four critical-control criteria. Examples include training, procedures, permits, supervision and alarms that need a person to respond.	"Supporting" does not mean optional, unimportant or unnecessary. Supporting controls may be essential, need clear expectations and checking, and their failure may require work to stop. A supporting control does not become critical because it is the strongest control currently available.
Control effectiveness	Whether the design of a control is capable of providing the protective outcome required for the defined exposure and conditions, assuming it is implemented and used as intended.	A control must be capable of providing the protection required for the defined exposure and conditions. Verification then checks whether it is in place and meeting its defined performance requirements in practice.

Concept	Meaning	Why it matters / key qualification
Verification	Checking, in real work, that the required control is in place and meeting its defined performance requirements – or not.	Tests performance against the defined standard, not just presence. Identifies missing or ineffective protection before harm occurs.
Monitoring	Looking across verification findings and other relevant evidence over time to understand how critical controls are performing and identify emerging, recurring or systemic weaknesses.	Individual verification findings show control performance at the point checked. Monitoring looks across the wider evidence for patterns requiring leadership attention and action.
Assurance	A competent and sufficiently objective second look at the control-performance and verification evidence, including through independent sample checks, to judge how much confidence leaders and officers can place in it.	Does not replace operational ownership or routine verification. Confidence is a judgement about the evidence, not a pass rate.
High potential incidents	Incidents with credible potential for serious harm, whether or not harm occurred.	Directs organisational attention to events that could credibly have killed or caused serious harm.
"Failed safely" / "failed lucky"	Learning prompts for high potential incidents: **Failed safely:** a critical control was in place, performed its defined protective function, and prevented a serious-harm outcome. **Failed lucky:** a critical control was absent or ineffective and serious harm was avoided by chance. **Not established:** the evidence is insufficient to say which.	Helps distinguish whether serious harm was prevented by effective controls or by chance, based on the protective function that actually prevented it. Section 7 provides an example.

Restricted Content

4. Accountability, Leadership, and Assurance

Good Critical Risk Management depends on clear accountability across the full cycle: identifying and assessing critical risks, selecting and implementing controls, verifying performance, responding to weakness, and improving the system. This section describes the functions that need to be performed and the competence they require, rather than prescribing departments, job titles or a single organisational structure. Responsibilities should be assigned to people with the authority, resources, and competence to act.

Who manages critical risks – and who supports them

Critical risks arise from work activities and operational decisions – meaning the people who own the effective management of critical risks are operational leaders, managers, supervisors, and workers:

- **Operational leaders, including executives:** accountable, within their authority, for critical risks being effectively identified; reasonably practicable controls being resourced and effectively implemented; sufficient high-quality verification being completed; verification findings and other relevant evidence being monitored for emerging, recurring or systemic weaknesses; and gaps and weaknesses being effectively addressed.
- **Operational managers and supervisors:** accountable for controls being applied and checked before work starts; actively verifying that controls are in place and meeting their performance requirements; and escalating concerns or resource needs.
- **Workers:** apply controls, report weaknesses, and contribute to risk identification and improvement.

When operational ownership is weak or unclear, critical risks and controls can be incorrectly treated as the responsibility of others - such as an H&S team - to source, implement, or manage. Verification of controls can also wrongly be viewed as a safety task imposed onto operational teams rather than a core part of normal operational work, and operational decisions can weaken controls without the consequences being understood.

Operational ownership works best when it is supported by people with competence relevant to the particular critical risk. Support, advice and constructive challenge may come from H&S professionals, engineers, occupational hygienists, process safety specialists, or other competent people, whether employed by the PCBU or external. They provide technical advice, help leaders understand the risks, coach and constructively challenge how much confidence operational and senior leaders should place in operational checks and reporting. Providing support does not transfer ownership of critical risks, controls, or routine verification activities to those providing it.

Five functions matter. They may be performed by different people or teams, or combined, depending on the PCBU:

- Lead and govern: officers and senior leaders set expectations, provide resources and seek evidence that critical risks are effectively managed.
- Own, manage, verify, and monitor: leaders and operational teams manage critical risks and controls, verify them in real work, monitor findings and other evidence for patterns and weaknesses, and respond to gaps.

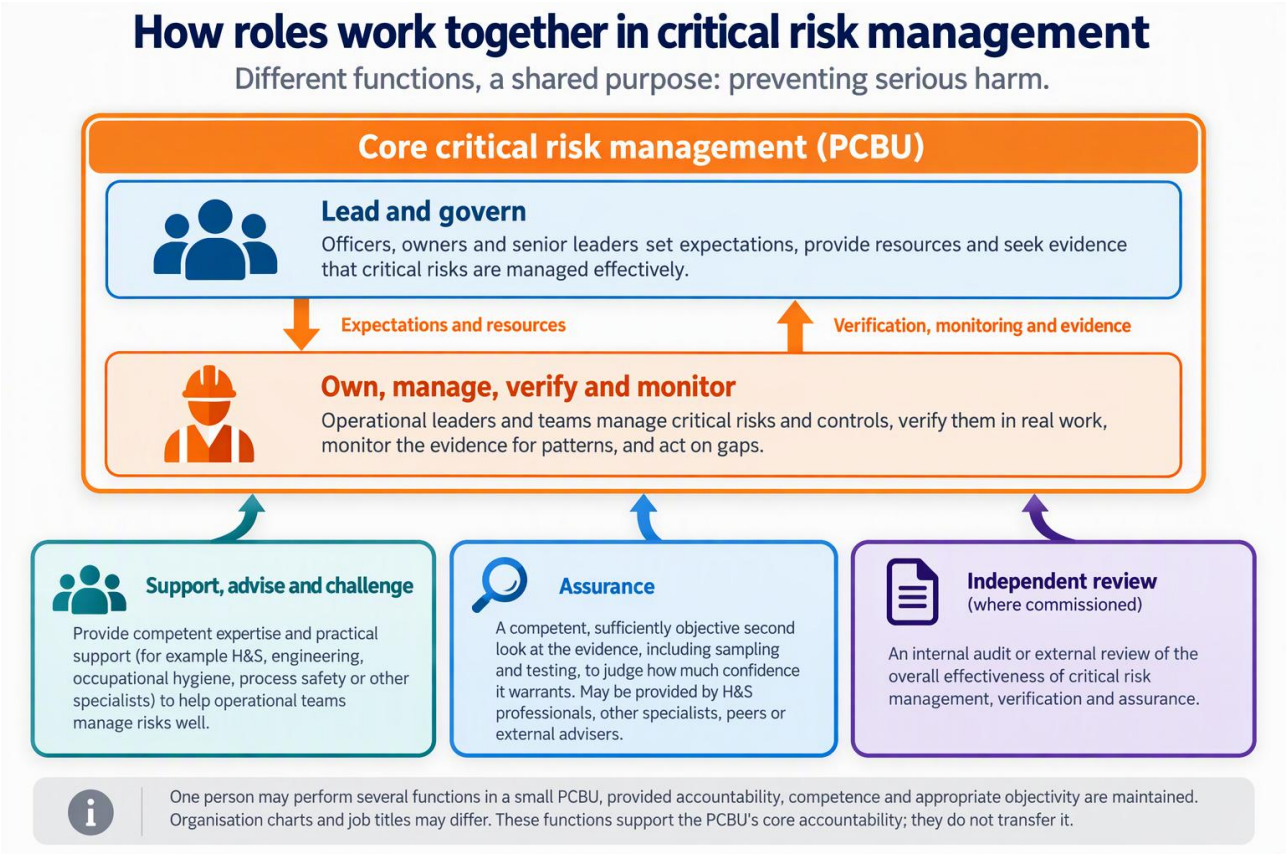
Restricted Content

- Support, advise and challenge: competent people provide technical expertise, advice, coaching and constructive challenge.
- Assure: a competent and sufficiently objective second look at the control-performance and verification evidence, which may be provided by H&S professionals, other technical specialists, a competent peer or an external adviser, to judge how much confidence it warrants.
- Review independently (where commissioned): internal audit or external review of critical risk management arrangements, including operational verification and assurance.

Each function needs people whose competence matches the critical risk concerned. Competence in health and safety generally does not automatically provide the technical authority to design, approve, verify or assure controls for every risk (see Section 8). In a small PCBU, one person may perform several functions, provided accountability, competence and appropriate objectivity are maintained. A larger PCBU may allocate them to different roles, teams or external providers. This guide does not require any particular structure.

Where duties overlap between different PCBUs, those PCBUs should consult, cooperate and coordinate to manage shared critical risks. They should agree who establishes, maintains and verifies controls, and how gaps are escalated and addressed. Allocating activities does not transfer legal duties; each PCBU remains responsible to the extent of its influence and control.

The diagram below shows how these functions relate. It describes responsibilities, not an organisation chart. Organisational structures differ, and a small PCBU may combine several functions in one person.



Restricted Content

Worker engagement and participation

Workers often have the clearest understanding of how work is done, where controls are difficult to use, and how conditions, pressures, or workarounds can weaken those controls. Meaningful worker engagement is therefore both a legal duty and a critical enabler of effective Critical Risk Management.

PCBUs should engage directly affected workers when identifying critical risks, selecting or changing controls, defining performance requirements, designing verification, and learning from events. They should share relevant information, allow reasonable opportunities to contribute, consider workers' views, and communicate decisions.

Worker engagement, including where it involves Health and Safety Representatives, does not transfer the PCBU's legal duties or operational leaders' accountabilities onto those workers or Representatives. Workers retain responsibilities relevant to their roles; their participation improves decisions by bringing work as performed into the design, verification and improvement of critical controls.

Critical Risk Governance

Governance of a PCBU is undertaken by its officers, who have specific and personal legal duties relating to due diligence. They should seek evidence that the PCBU understands its critical risks and maintains effective controls to prevent serious harm so far as is reasonably practicable.

In their governance capacity, officers establish expectations, oversee resourcing, and seek evidence that critical controls are in place and working effectively. The same person – such as an owner-manager, partner, or chief executive – may also carry operational management responsibilities. These are distinct functions, not necessarily separate people or organisational layers.

Officers should take reasonable steps to:

- understand and keep up to date with the PCBU's operations, its critical risks, and relevant health and safety matters; and
- verify that:
  - critical risks have been effectively identified and are being prioritised;
  - critical controls are clearly defined and resourced appropriately;
  - critical controls are effectively verified in practice;
  - material control gaps and weaknesses are effectively identified and escalated; and
  - learning leads to sustained and meaningful improvement.

Officers should not treat general health and safety activity measures, compliance reports, general audit results, statements of leadership commitment or intent, or consistently green dashboards as evidence of effective critical risk management.

This guide does not reproduce wider health and safety governance guidance. Officers should use current New Zealand governance guidance – particularly the Institute of Directors / WorkSafe 2024 *H&S Governance Good Practice Guide* – alongside this guide when determining how they will exercise oversight and seek assurance.

Restricted Content

Critical Risk Leadership

Leadership turns governance expectations into operational practice through the priorities leaders set, the decisions and trade-offs they make, and the behaviours they reinforce.

Effective leaders:

- make critical risk responsibilities clear and keep critical risks visible in planning and operational decisions;
- seek evidence that controls remain effective, that verification is meaningful and adequately resourced, and that findings are monitored for emerging, recurring or systemic weaknesses;
- encourage early, transparent reporting of control weaknesses and respond decisively when controls are absent, degraded or ineffective; and
- act on learning so that it leads to sustained improvement.

Leaders should create an environment where raising concerns is publicly recognised as a positive contribution to safety, and concerns are acted on before harm occurs.

Operational leaders and teams are accountable for managing critical risks and controls, carrying out routine verification, monitoring what the evidence shows across their work, and responding to gaps and weaknesses. Assurance provides a competent and sufficiently objective second look at the evidence. Section 7 explains verification, monitoring and assurance, and their relationship to control effectiveness; Section 9 explains reporting and interpretation.

Restricted Content

5. Identifying and Assessing Critical Risks

Identify critical risks through both HSWA routes described in Section 2: risks associated with Schedule 1A hazards, and risks associated with other hazards that meet the statutory criteria for serious outcomes.

Identify critical risks

Cover immediate harm, catastrophic events – those with the potential for kill multiple people at once – and illness from repeated or prolonged exposure. Consider actual routine and non-routine work, including maintenance, shutdowns, abnormal conditions and interfaces with other PCBUs.

Draw on technical and operational knowledge, worker and contractor insight, industry experience, incidents and verification findings. Validate the profile with workers, contractors and frontline leaders to identify missing exposure pathways.

Group similar risks or pathways where useful, but do not impose an arbitrary numerical limit. The aim is a manageable critical risk profile that supports effective controls and verification—not an undifferentiated hazard list.

Useful test for hazards outside Schedule 1A: If a person were exposed to this hazard and the controls failed, would death, serious injury or illness, a notifiable incident, or a listed occupational disease be a likely consequence?

Remember: Risks associated with Schedule 1A hazards need no additional severity test. Infrequent incidents, apparently effective controls or favourable injury results do not remove a risk from the critical risk profile.

Describe exposure pathways

For each critical risk, PCBUs should describe how a specific hazard could reach or affect a person and cause serious harm, rather than simply name the hazard. This includes immediate harm as well as ill-health from repeated and/or prolonged exposure. For example, *'mobile plant*' is a hazard; '*person struck by moving mobile plant*' is an exposure pathway that could credibly lead to serious harm (see illustrative example in diagram below).

Using explicit exposure pathways makes control selection easier and more effective; listing hazards does not. Section 6 explains control selection, and Appendix A provides further illustrative exposure pathways and work contexts.



Assess control needs

PCBUs should use the exposure pathways to establish what specific protection is needed to prevent or mitigate serious harm, and where that protection could fail.

The assessment should be proportionate to the risk and the context of the PCBU's work. PCBUs should not use a risk matrix or arbitrary risk score to determine whether a risk is critical or to downplay a low-frequency serious harm scenario. The implementation toolkits provide assessment methods and tools.

Risks that are not critical

Non-critical risks are those that do not meet either of the critical risk thresholds. Large PCBUs must manage them as well as critical risks, but must prioritise critical risks; small PCBUs' main risk management duties generally apply only to critical risks (Section 2).

Restricted Content

6. Selecting and defining critical controls

PCBUs should select the most effective controls that are reasonably practicable; identify which meet the criteria for a critical control; define how they must perform; and protect them through operational decisions and change. A control does not need to be designated as "critical" to be important or reasonably practicable.

PCBUs should implement the combination of controls needed to eliminate or minimise risk so far as is reasonably practicable, not only those designated as critical.

Use the hierarchy of controls

The hierarchy of controls should guide the selection of controls for critical risks. PCBUs should first assess whether there is a reasonably practicable way to eliminate the specific critical risk. Where elimination is not reasonably practicable, they should assess the available options for minimising by moving progressively down the hierarchy and adopting the most effective combination of controls that is reasonably practicable for the specific exposure pathway.

'Higher-order controls' are those that eliminate the risk or act directly on the hazard or exposure pathway through substitution, isolation, or engineering interventions. 'Lower-order controls' are those that generally depend more heavily on human behaviour, such as applying procedures and personal protective equipment.

Assess whether the proposed controls will be effective

PCBUs should assess whether each proposed control can provide the intended protection under the demands and conditions in which it will be used. For controls being considered as critical, this includes sufficient capacity to prevent the defined exposure from causing serious harm – not merely reduce exposure to some extent. The assessment should address foreseeable failures, dependencies on other controls or systems, and applicable technical requirements. Complex risks, including process safety risks, may require competent specialist analysis to establish an adequate design.

Correct implementation and use cannot compensate for inadequate control design.

Control selection and performance requirements should be tested with the workers who would be required to use, maintain, or work around the control, alongside relevant operational and technical expertise. Their insight can identify practical dependencies, foreseeable workarounds, and conditions that may not be apparent from design documentation alone.

Determine what is reasonably practicable and justify control selection

Decisions about what is reasonably practicable should draw on the assessment of risk and control effectiveness and address the full combination of controls – not only those designated as critical. A PCBU's current practices, preferences, risk appetite, or budget cannot, on their own, determine what is reasonably practicable. The assessment should consider what is known, or ought reasonably to be known, about the risk and available controls, drawing on legislation, Approved Codes of Practice, regulator guidance, recognised standards, industry good practice, and relevant technical knowledge.

Restricted Content

PCBUs should not use internal risk scores or investment thresholds to rule out more effective controls. A low estimated likelihood or an “acceptable” matrix rating does not, by itself, show that further controls are not reasonably practicable.

Cost should be considered last, after assessing the risk and which controls are available and suitable. Cost alone can only justify not adopting a control if the cost is grossly disproportionate to the risk. A control should not be rejected solely because it is expensive or exceeds the budget.

If PCBUs do not adopt reasonably available higher-order controls, they should record the main reasons, the evidence supporting the decision, and how they will control the risk that remains. The level of detail should be proportionate to the risk.

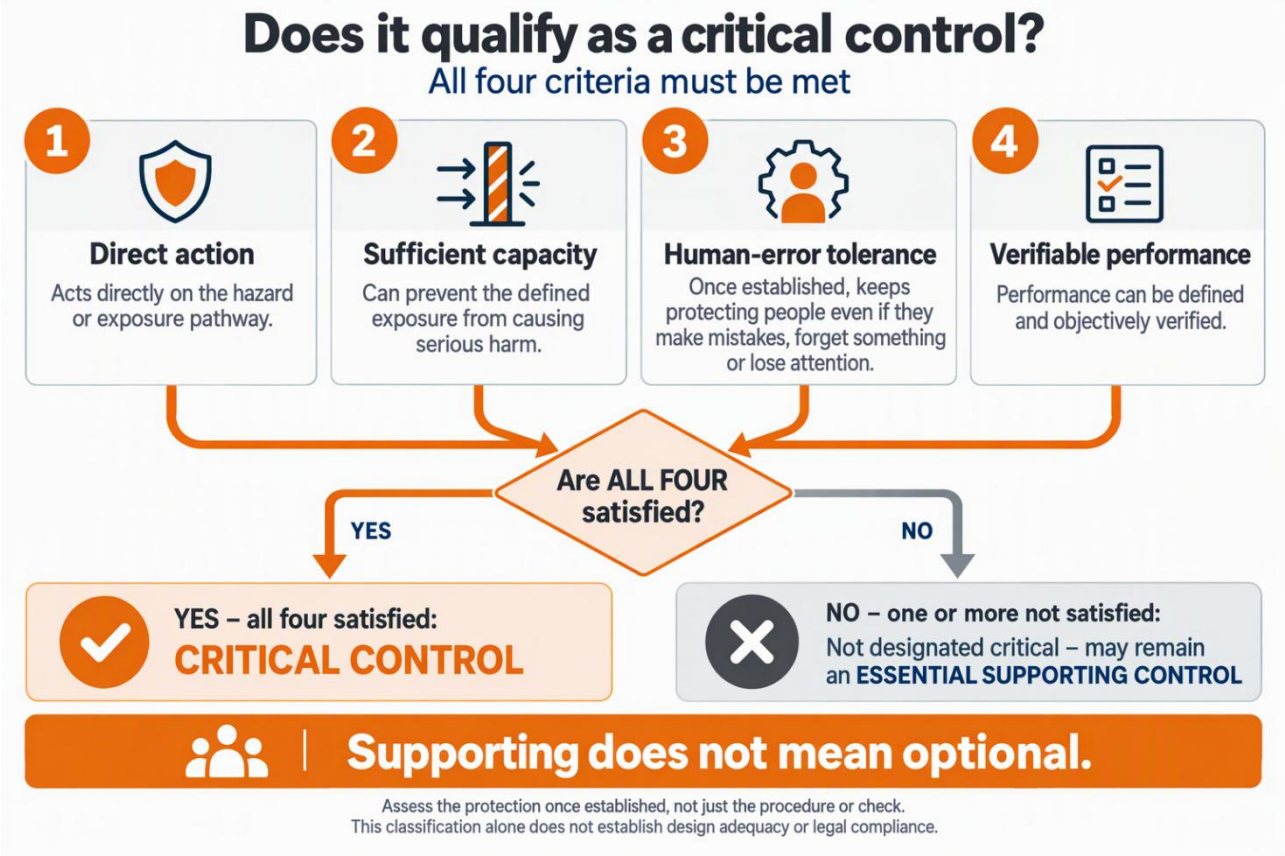
Recording the decision does not, by itself, demonstrate that the risk has been minimised so far as is reasonably practicable. PCBUs should establish, using suitable evidence, that the selected combination of controls will provide the required protection. If protection is inadequate or effectiveness remains uncertain, they should resolve the gaps and reconsider the control options before relying on them.

Identify the critical controls

PCBUs should assess each control’s intended protective function and design against the four criteria below. Position in the hierarchy alone does not determine critical status.

Under this guide, a control qualifies as critical only if it meets all four criteria:

- It acts directly on the hazard or exposure pathway.
- It has sufficient capacity to prevent the defined exposure from causing serious harm.
- Once established, it is designed to keep protecting people even if they make mistakes, forget something or lose attention during the work.
- It has performance that can be defined and objectively verified.



These criteria define a critical control for this guide; other frameworks may use the term differently. The designation alone does not establish sufficient protection or legal compliance.

A critical control must withstand the hazard and conditions it is designed for. Reducing exposure or harm is insufficient if the defined exposure could still cause serious harm.

People are still needed to establish, install, maintain and check a critical control. Criterion 3 concerns the protection once the control is established: it must not depend on every human action being correct. For example, a secured physical isolation that keeps protecting even if someone tries to start the equipment can qualify; the permit, procedure and tags that support it cannot qualify on their own.

Training, procedures, permits, supervision, and signs or alarms that depend on a person responding are supporting controls, because their protection relies on people responding correctly. “Supporting” does not mean optional, unimportant or unnecessary: supporting controls may be essential. They need clear responsibilities and performance expectations, effective implementation and checking, and restoration when ineffective, and their failure may require work to stop.

A missing or ineffective critical control remains critical. A supporting control does not become critical merely because it is the strongest control currently available, and the criteria are not relaxed for human-dependent controls. Either way, the overall combination of controls must still provide effective protection so far as is reasonably practicable.

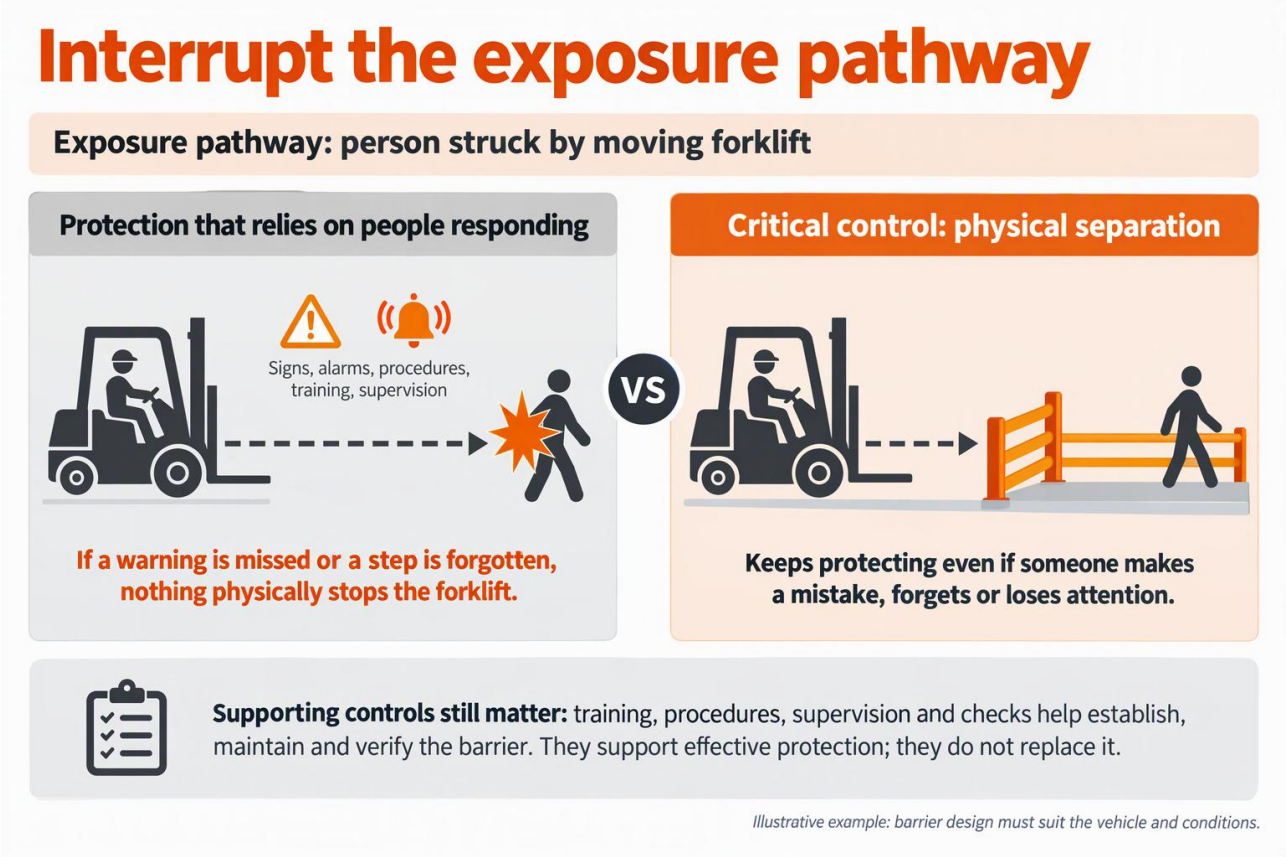
Where no control currently meets all four criteria, the PCBU should:

- assess whether the overall protection is adequate for the defined exposure, using competent advice where needed;
- make reliance on non-critical controls visible to its leaders and officers;

- prioritise improvements that establish a qualifying critical control where reasonably practicable; and
- not allow work to continue without effective protection. An improvement plan does not justify work without effective protection.

Examples of critical controls and supporting measures

The diagram below shows how a critical control effectively interrupts an exposure pathway.



The table below provides further examples of critical vs supporting controls. Control types do not qualify as critical by name alone; each must meet the criteria for its defined exposure.

Critical Risk	Critical Control	Supporting controls
Person falls from height	Edge protection, guardrails, or engineered fall prevention system	Signs, instructions to stay away from the edge; competence to select and use the fall-protection system
Contact with moving machinery	Interlocks, guarding	Signs and standard operating procedures
Person struck by moving vehicle	Physical barriers separating people and vehicles	High-visibility clothing; proximity alarms that require a person to respond; a 3m exclusion rule around moving forklifts

Critical Risk	Critical Control	Supporting controls
Person exposed to uncontrolled hazardous energy	Effective energy isolation that prevents hazardous energy reaching the work	Permit, isolation procedure, signage and competence
Person exposed to fire, explosion or fragments when overpressure ruptures a process vessel and releases flammable contents	Independent automatic shutdown or engineered pressure relief with safe discharge. Each must meet all four criteria, including sufficient capacity to prevent serious harm from the defined overpressure exposure.	Operating procedures and operator competence; high-pressure alarms requiring human response; inspection, maintenance and proof-testing arrangements that sustain and verify the protective systems
Person exposed to hazardous noise from plant or equipment over time, causing permanent hearing loss	Engineered elimination or enclosure of the noise source that reduces exposure below harmful levels, where competent assessment shows it meets all four criteria	Hearing protection, work rotation, signage and training; noise monitoring and health surveillance that confirm exposure is controlled

Appendix B shows how all four criteria apply to selected exposure pathways, including the conditions and evidence needed for a control to qualify.

Define control performance and ownership

For each critical control, PCBUs should define:

- **roles and accountability:** who is accountable for, and who carries out, setting and approving control performance requirements; implementing or making the control available; applying it in practice; and verifying that it is present and meeting its performance requirements.
- **technical basis:** evidence that the control meets all four critical-control criteria
- **required performance:** the protection and performance standards required, the conditions it must work in, and when it must be in place or available – including abnormal conditions.
- **verification:** how and when performance will be verified
- **response:** what must happen if performance requirements are not met.

These arrangements should suit the PCBU's critical risks, size, and complexity. One person may perform several of these roles in a small PCBU; a larger PCBU may assign them to different roles, teams, or functions. The implementation toolkits provide detailed methods and tools.

Embed critical risks and controls in systems and decisions

PCBUs should build critical risk and control requirements into everyday planning, approval and operational systems – not treat them as a separate health and safety process. This includes

design, procurement, project delivery, resourcing, maintenance, and contractor arrangements.

Before approving decisions that could affect exposure to critical risks or effectiveness of critical controls, PCBUs should engage affected workers, assess the implications, and establish how effective protection will be maintained. Decision makers should understand the critical risk exposure that will remain.

These checks should cover permanent, temporary, and gradual changes to work, conditions, interfaces, responsibilities, resources, or underlying assumptions.

Any alternative protection must be agreed and resourced, then put in place and verified before affected work starts or continues. Confirm that controls remain effective after implementation.

Operational systems should prevent work from proceeding without effective protection, including any critical controls required for the work.

Restricted Content

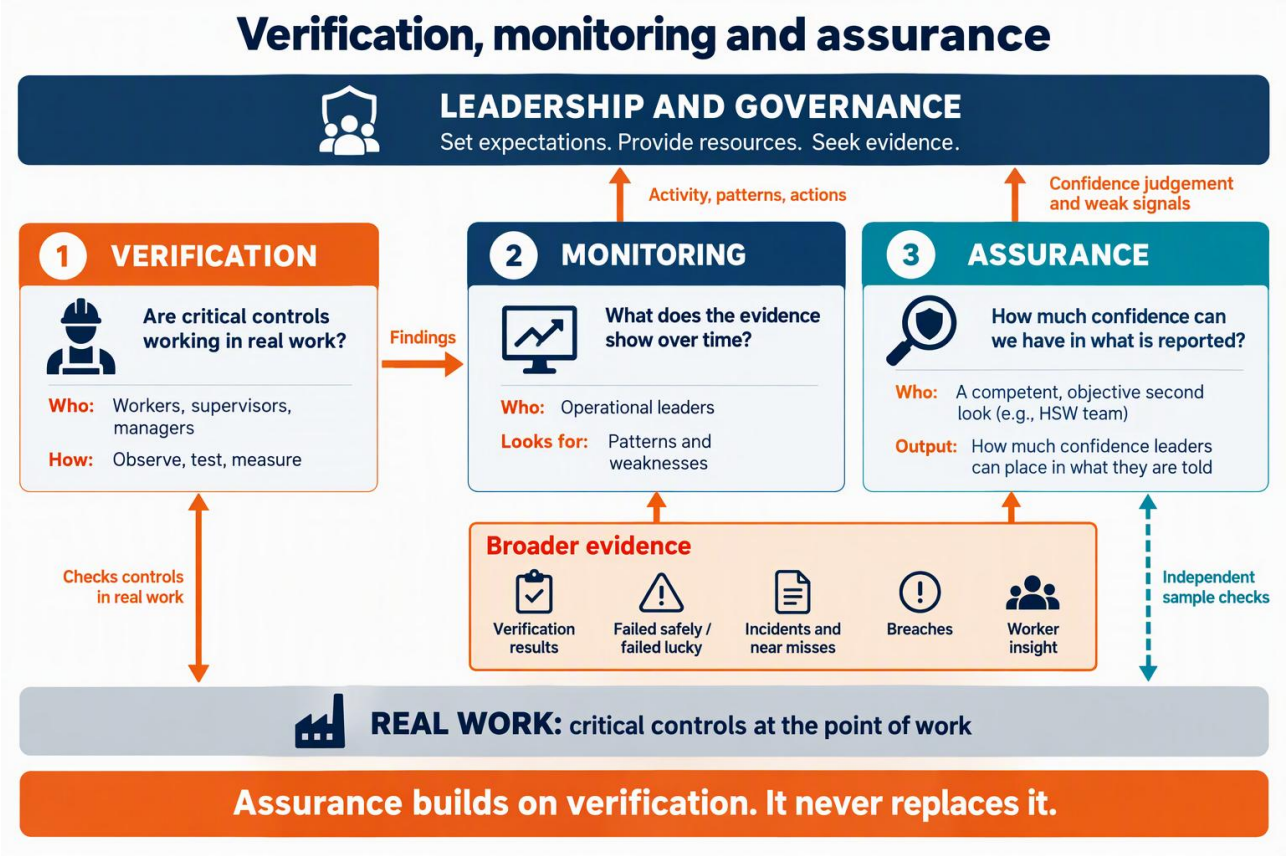
7. Critical control verification, monitoring and assurance

Why verification matters and what it must establish

These arrangements should suit the PCBU's critical risks, size, and complexity. One person may perform several of these roles in a small PCBU; a larger PCBU may assign them to different roles, teams, or functions. The implementation toolkits provide detailed methods and tools.

Concept	The question it answers	Who and how
Control Effectiveness	Is the design of the control capable of providing the protective outcome required for the defined exposure and conditions?	Established through competent assessment of the control's design, capacity and required performance for the defined exposure and conditions. Verification provides evidence that those requirements are being achieved in practice.
Verification	Is the required control actually there, and is it meeting its defined performance requirements in the real work?	Operational workers, supervisors, and managers test performance against the defined standard through observation, testing, or measurement. Presence alone is not verification.
Monitoring	What do verification findings and other relevant evidence show about control performance across the work and over time?	Operational leaders – including senior leaders – monitor patterns across verification findings and other relevant evidence to identify emerging, recurring, or systemic weaknesses and determine where action is needed.
Assurance	How much confidence should leaders and officers place in the evidence and the conclusions drawn from it?	A competent and sufficiently objective second look at the evidence and the conclusions drawn from it, including sample checking and constructive challenge.

The diagram below shows how verification, monitoring and assurance differ, which evidence each draws on, and how monitoring and assurance both report to leadership and governance.



Proportionality in practice: the same concepts apply to every PCBU, but arrangements should reflect its size, complexity and critical risks.

In a small PCBU	In a large PCBU
The owner or supervisor checks key controls in the field, watches for recurring weaknesses, and acts on gaps. An occasional competent second look tests whether those checks and conclusions can be trusted.	Structured operational verification covers critical controls across sites. Leaders monitor findings and other evidence for patterns and systemic weaknesses. Specialists advise on control effectiveness where needed, and separate assurance tests the evidence and conclusions.

Verification responsibility

Routine verification is part of managing operational work. Those carrying out and supervising work are responsible for checks relevant to its critical risks.

Within the areas they oversee, leaders – including senior leaders – are accountable for verification that:

- is adequately resourced and carried out by competent people;
- provides reliable evidence of control performance, with appropriate check volumes and coverage; and
- leads to timely action that maintains or restores protection.

Leaders should monitor verification findings alongside other relevant evidence to identify patterns, recurring weaknesses and systemic issues requiring action.

Restricted Content

Section 4 explains operational ownership and competent support.

Verification: checking that critical controls work

The primary focus of verification should be weighted towards critical controls. Its extent and frequency should reflect the specific critical risk, the specific control/s, and any changes to operating conditions, with sufficient coverage of the work requiring protection. PCBUs should check supporting controls where their failure could undermine critical controls or overall protection, without displacing the focus of verification towards critical controls.

Verification methods should establish whether the control meets its performance requirements in practice and when needed, including non-routine work. Combine observation, testing or measurement with worker insight into normal, abnormal and changing conditions to identify difficulties, adaptations and weakening protection.

Verification is therefore more than confirming that something is present. It tests performance against the defined standard – for example, not only that a barrier is installed, but that it is intact, correctly positioned and stopping the movement it is required to stop. A completed checklist, or the presence of a control, does not on its own verify its performance.

Monitoring: what does the evidence show over time?

Monitoring looks across verification findings and other relevant evidence over time to identify emerging, recurring, or systemic weaknesses. Relevant evidence may include observations, failures and breaches, high potential incidents and near misses, inspection, testing and maintenance records, worker insight and, for health risks, exposure measurement and health surveillance. Test whether these sources tell a coherent story: very high verification pass rates deserve scrutiny where other evidence shows repeated weakness in the same protective function. Investigate differences rather than assuming the cause, and act where protection may be weakening.

Assurance: a competent second look at the evidence

Assurance is a competent and sufficiently objective second look at the verification evidence, how it is being monitored and interpreted, and the conclusions being reported. It may be provided by H&S professionals, engineers or other specialists, a competent peer or an external adviser. Those providing assurance need competence relevant to the critical risk and must not be responsible for the routine verification being assessed.

Those undertaking and providing assurance should:

- assess the quality, coverage, methods and findings of operational verification;
- test whether material patterns, conflicting evidence and recurring weaknesses are being recognised and addressed;
- compare operational findings with their own sample-based checks and investigate significant differences; and
- report how much confidence the evidence, operational monitoring and conclusions warrant.

In a smaller PCBU, assurance could involve reviewing a sample of verification records, comparing them with conditions observed at work, and assessing the response to weaknesses.

Restricted Content

General health and safety audit results do not, by themselves, establish critical-control effectiveness.

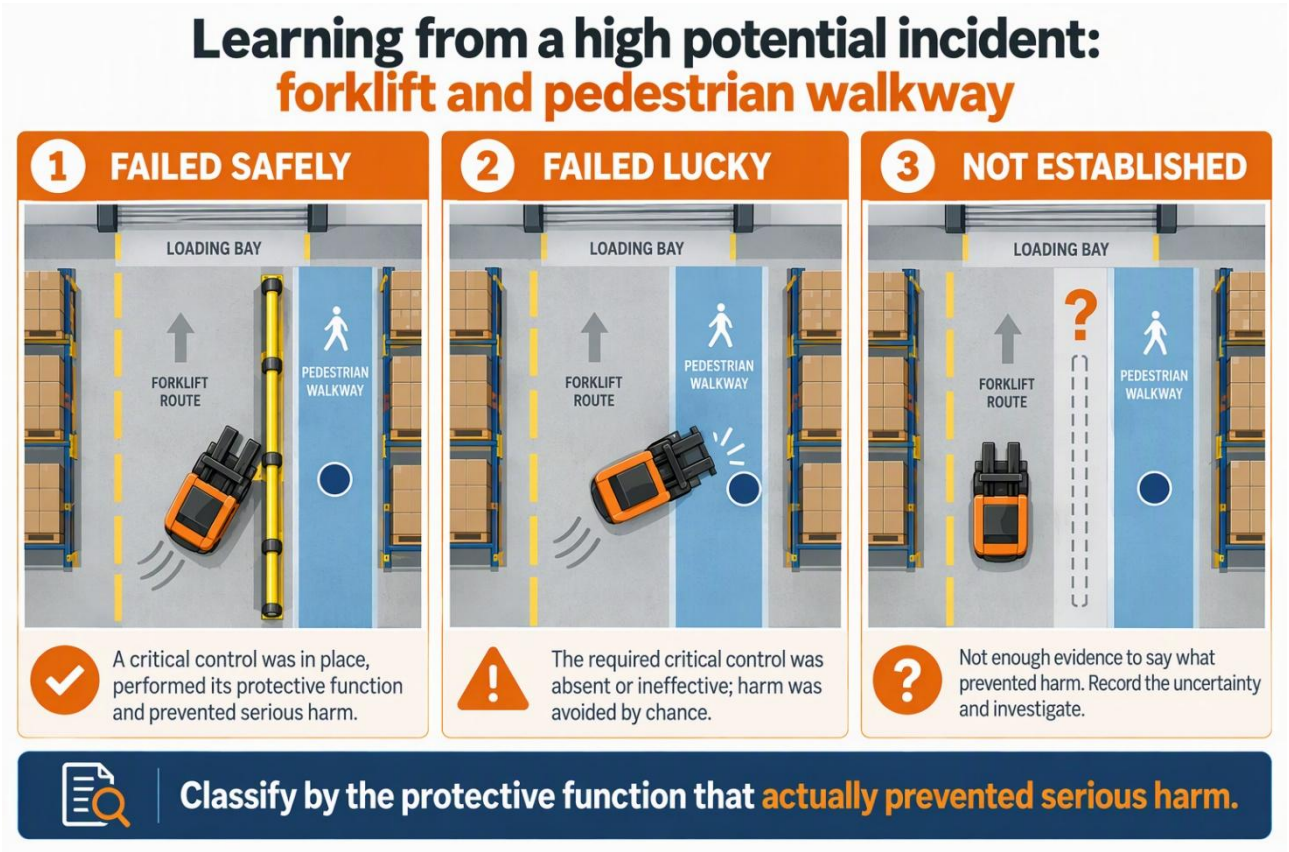
Leadership or governance may also commission internal audit or an independent external review to assess the effectiveness of critical risk management arrangements, including operational verification and assurance.

Interpret evidence from high potential incidents

High potential incidents show how controls perform when they are challenged. Considering what actually prevented serious harm gives PCBUs a useful additional way of learning about control performance. “Failed safely” and “failed lucky” are learning prompts, not scores, and some events cannot be classified:

- **Failed safely:** a high potential incident in which a critical control was in place, performed its defined protective function, and prevented a serious-harm outcome.
- **Failed lucky:** a required critical control was absent or ineffective and serious harm was avoided by chance.
- **Not established:** there is insufficient evidence to say which protective function, if any, prevented serious harm. Record the uncertainty and investigate; do not force the event into either category.

Example: A forklift veers towards a pedestrian walkway while a worker is nearby. If the fixed barrier stops entry, the event “failed safely”; if no effective barrier was present and harm was avoided by chance, it “failed lucky”; if the evidence cannot establish what prevented harm, the finding is “not established” and should be investigated (see below).



Restricted Content

Classify an event by the protective function that actually prevented serious harm, not simply by whether anyone was hurt or which control was intended to protect people. A “failed safely” event still warrants review; a “failed lucky” event is a serious warning about missing protection. Use this learning alongside verification findings and other evidence to identify recurring or systemic weaknesses and challenge the broader picture of control performance. Incident learning is reactive and should remain distinct from proactive verification; do not use it as a measure of overall performance.

Because classification involves judgement, it should be made or reviewed by someone competent in the critical risk who is not responsible for the result being reported, using consistent criteria and recording the basis for each classification. Trending the proportion of events that “failed safely” can encourage favourable classification, so treat the rate as a prompt to review the evidence, not as a target.

Act on findings

Verification, monitoring and assurance findings should lead to timely action. Where a required critical control is missing or ineffective, affected work should not start or continue until protection is restored or an effective alternative is authorised and verified. Failure of a necessary supporting control also requires work to stop where effective protection can no longer be assured.

Where it cannot be established whether a required control is effective, PCBUs should not assume that it is. They should investigate promptly and, where effective protection cannot be assured, treat the situation as a control failure.

The implementation toolkits provide practical approaches to verification, monitoring, and assurance.

8. Capability

Capability means being able to do what a role requires, not simply completing training. People should understand how serious harm could occur in work they perform, supervise, or influence; which controls are most important in protecting them or others; the performance requirements relevant to their responsibilities; and what to do when protection weakens. Leaders and other decision-makers should understand how their decisions affect controls.

Capability expectations should reflect each role's influence on critical risks and controls. Particular attention should be given to those who authorise work; make resource- or change-related decisions; supervise critical risk exposure; design or maintain controls; verify performance; or are required to respond when operating conditions change.

Capability must be relevant to the particular critical risk. People who perform risk-specific tasks, make control decisions, or carry out verification or assurance need the technical, trade or specialist capability that the risk demands, including refresher or re-confirmation where skills or conditions change. General health and safety competence does not automatically provide the technical authority to design, approve, verify or assure controls for every critical risk; where it does not, the relevant specialist should be involved.

PCBUs should confirm capability through observation and practical demonstration suited to the role, including realistic abnormal conditions where appropriate. Supervision, verification findings, event learning, and operational changes should inform learning needs and help establish whether capability is maintained.

Capability can erode as work, controls, systems, workload, or personnel change. PCBUs should review relevant capability when verification identifies gaps or work changes, rather than rely only on scheduled refresher training. Leaders should provide time for learning, resource controls, and respond constructively to concerns.

Useful test: How does the PCBU know people can apply the requirements relevant to their roles, and what evidence would reveal weakening capability?

Restricted Content

Restricted Content

9. Measurement and reporting

Tracking, monitoring and reporting on critical risk management should help PCBUs decide where to act and why. They should show exposure to critical risks, how critical controls are performing, emerging weaknesses, and whether action is strengthening protection. They also help officers fulfil their duty to verify that critical risks are being managed effectively.

Measuring and reporting what matters

Injury rates, general health and safety activity counts, and leadership commitment to safety do not, by themselves, demonstrate effective control of critical risks. PCBUs should focus on proactive evidence of control performance, complemented by incident findings that may reveal weaknesses missed by routine verification.

Reporting to senior leaders and officers should centre on operational teams' critical control verification activity and findings, together with what monitoring of those findings and other relevant evidence shows. Operational leaders should present and explain the results for their business areas, including what was assessed, material patterns and weaknesses, what the evidence supports, and how gaps are being addressed.

Those providing assurance – a competent and sufficiently objective second look, which may come from H&S professionals, engineers or other specialists, a competent peer, or an external adviser – should provide a complementary test-and-challenge perspective. They should explain how much confidence the evidence, operational monitoring and reporting warrant, and why. The detail should be proportionate to the critical risks and decisions required.

The figure below shows six dimensions that good critical control reporting should cover. The first three describe the evidence: what was checked, how well the checks cover the work, and what verification found. The last three support decisions: what monitoring shows across the evidence, whether action restored and improved protection, and how much confidence the evidence warrants.



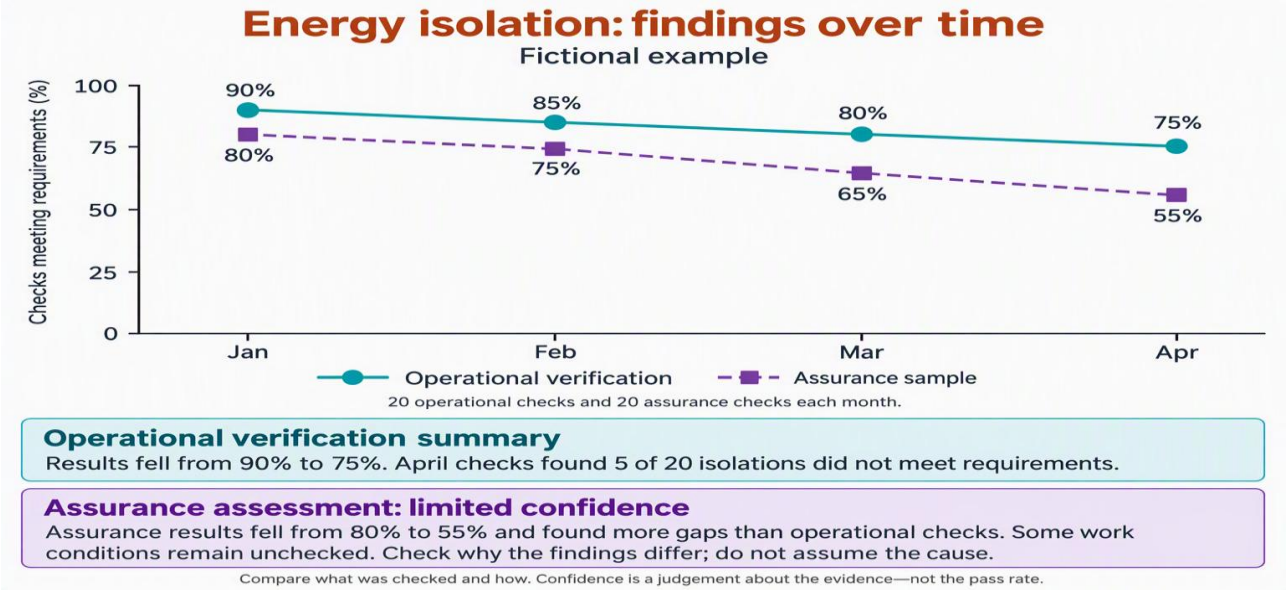
Proactive verification and high potential incident learning provide different but complementary evidence. Monitoring considers these and other relevant evidence together for patterns and weaknesses; assurance tests how much confidence the evidence and conclusions warrant. Do not blend them into a single score. Incident findings are reactive and should remain distinct from proactive verification results; reporting should show what incidents reveal about critical control performance, including “failed safely”, “failed lucky” and “not established” findings (see Section 7). Trends can inform improvement priorities but do not replace proactive verification.

Illustrative reporting examples (for organisations with sufficient scale and data)

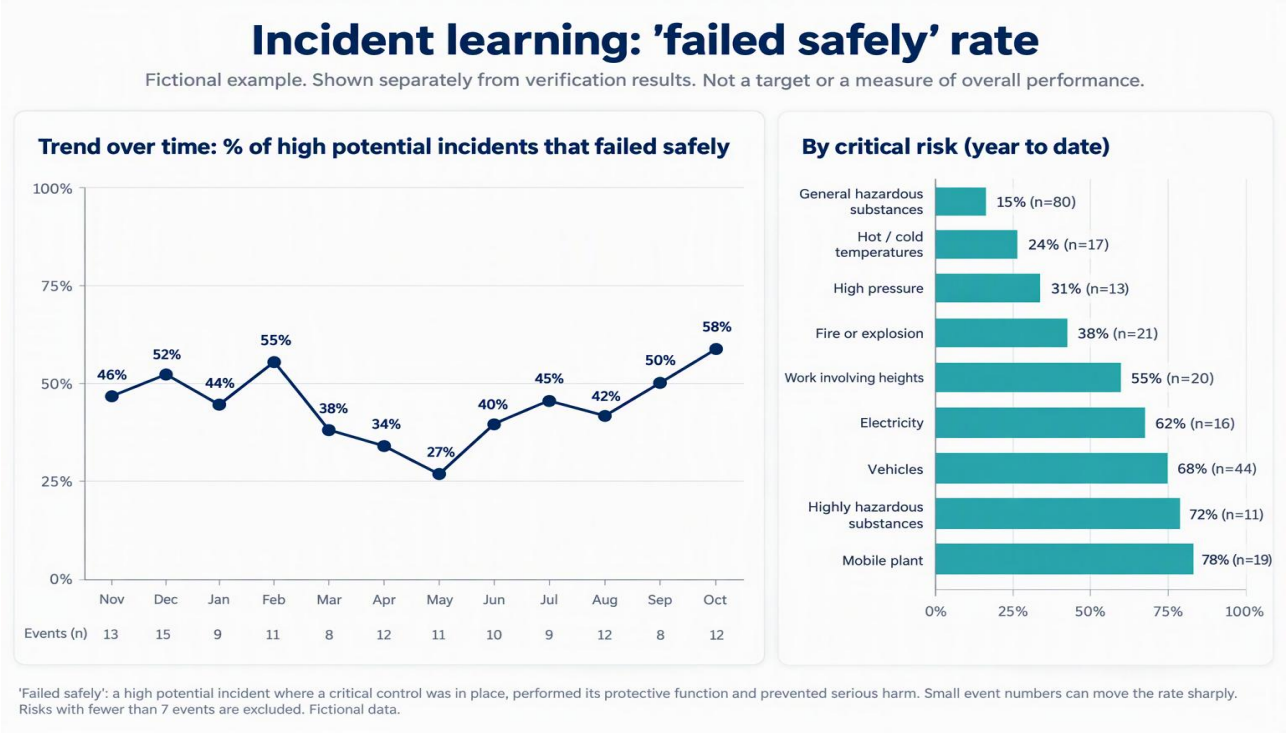
The three fictional examples below show one way verification, monitoring, and assurance evidence, and learning from high potential incidents, can be presented where a PCBU has enough scale and data to support this analysis, typically a larger PCBU with several sites or many checks. They are illustrations, not expected formats, and small PCBUs do not need to produce them. Each example uses separate fictional data, so figures are not comparable between examples. The implementation toolkits provide further examples.

Small PCBUs: where complexity is low, a simple record of significant findings, decisions, actions and whether they worked may be sufficient. Dashboards are not required?

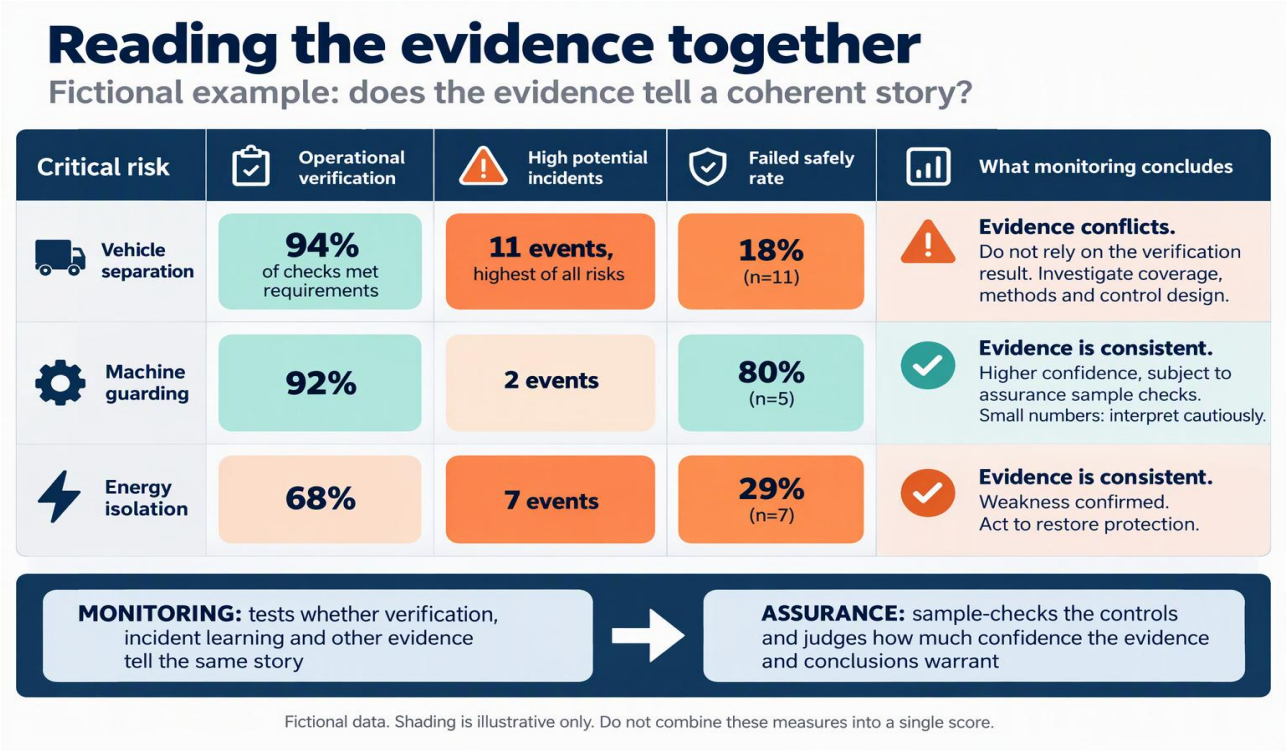
Example 1 shows how the performance of an individual critical control can be trended over time from two perspectives: what operational verification is finding, and what assurance sample checks find when they test the same control. Reading the two together shows whether they are tracking each other. A widening gap, or very high verification results that assurance cannot reproduce, is a prompt to investigate the reliability and coverage of verification, not to accept the result.



Example 2 shows how learning from high potential incidents can be reported as a trend in the proportion that “failed safely”, alongside the same measure for individual critical risks. It shows where direct controls are working when exposures occur, and which risks account for the weaker results. This is reactive evidence and is shown separately from proactive verification results. Trends can inform improvement priorities but should not be used as a measure of overall performance. A small number of events can move the rate sharply, so event numbers should be reported alongside it.



Example 3 builds on the first two examples to show why different evidence should be read together. It sets operational verification results, high potential incidents and "failed safely" rates side by side for three risks. For one risk, operational verification is strong, yet the same risk has the highest number of high potential incidents and a low "failed safely" rate. When the evidence conflicts, monitoring should treat the verification result with caution and investigate coverage, methods and control design, and assurance should sample-check the control. Where the evidence is consistent, whether strong or weak, confidence is higher. Do not combine these measures into a single score.



Restricted Content

Interpret results in context

Stronger verification and assurance may reveal longstanding gaps that were previously unseen. More reported weaknesses can therefore indicate better visibility, not necessarily deteriorating protection. The gaps still require action.

Conversely, consistently near-perfect results warrant scrutiny, particularly when incidents or other evidence conflict. Check that verification covers actual conditions, including non-routine work and night shifts, and that pressure for positive results is not distorting findings.

Interpret results in light of the controls and conditions assessed. Fixed guards may perform more consistently than controls for changing vehicle movements. Before comparing results over time, check whether the controls, conditions or methods have changed. Use these differences to target further checks and improvement – not to accept ineffective controls or lower protection standards.

Use reporting to support decisions and action

Reporting should be tailored to the audience and decisions required:

- operational teams need timely information about control gaps and actions they need to take;
- senior leaders need patterns, priorities, and resource implications; and
- officers need evidence that the overall approach is working and material weaknesses are being addressed.

Useful test: Does this reporting reveal emerging control weakness, increasing exposure or narrowing safety margins early enough for leaders to act before serious harm occurs?

10. Preventing drift in critical risk management

In critical risk management, *drift* is the gradual weakening of protection as changes build up in work, controls, or the systems that keep them effective**.** Change is not automatically drift. It becomes drift when controls become less effective or safety margins shrink.

Drift can develop when work changes faster than supporting systems, unsafe workarounds become normal, checks become less thorough, or leadership attention, resources, challenge and follow-through weaken or shift elsewhere. Because serious incidents are rare, this weakening may go unnoticed or unaddressed. No incidents can create false confidence even as controls become less reliable.

Drift does not necessarily mean people disregard safety. Leaders and workers may be responding to competing goals, operational pressures, changing conditions or poorly designed and resourced work. Decisions that seem reasonable individually can combine over time to weaken protection.

PCBUs should watch for changing assumptions, repeated control problems, workarounds and increasing reliance on supporting controls or individual judgement. Engage affected workers to understand why work is being adapted, and combine their insight with objective evidence to improve controls and the systems that sustain them.

Reviews should check whether:

- the critical risk profile still covers the work and exposures;
- controls remain effective under actual working conditions; and
- verification, capability, reporting and assurance are sufficient to identify and respond to emerging weaknesses.

Significant control failures, repeated problems, operational changes or declining confidence in critical controls should prompt review and action. Consider both the controls and the conditions in which they must work. **Do not delay action where effective protection is in doubt.**

Learning should lead to clear improvements in control design and reliability, work planning, resources, verification, capability or organisational decisions.

Useful test: Where could critical controls be weakening or becoming more dependent on workarounds, supporting controls or individual judgement, and how would we know?

Restricted Content

Appendix A: Examples of critical risks

These examples are illustrative, not a definitive list. PCBUs should apply both classification routes described in Section 5: identify risks associated with applicable Schedule 1A hazards and assess other hazards against the statutory criteria for serious outcomes. Exposure pathways should be described so that control needs are clear. A listed risk should not be excluded because events are infrequent or current controls appear effective.

Illustrative exposure pathway	Example work contexts
A person loses footing or support at height and falls to a lower level.	Roofs, scaffolds, elevated platforms, truck decks, ladders, excavations, towers, rope-access work and unprotected edges.
A moving vehicle or mobile plant enters a space occupied by a person and strikes or traps them.	Yard movements, loading, reversing, forklifts, public roads and work beside live traffic.
A collision or rollover exposes vehicle occupants to impact forces, crushing or ejection.	Operation of light, heavy or specialist vehicles, including vehicles towing loads or operating on unstable terrain.
A suspended load swings or drops, or stored material falls, into an area occupied by a person.	Cranes, hoists, rigging, loading, unloading and elevated stored materials.
A person or their clothing reaches moving plant parts, or plant movement traps them against another surface.	Conveyors, mixers, rollers, presses, packaging equipment and rotating or automated plant.
Unexpected energisation or release of stored energy reaches a person working on or near the equipment.	Maintenance, cleaning, de-jamming, fault-finding, commissioning and work involving stored pressure, pressure vessels or other energised systems.
Contact with an energised part allows electrical current to pass through a person, or an electrical arc exposes them to intense heat and pressure.	Energised work, testing, fault-finding, switchboards, low- and high-voltage equipment, and overhead or underground services.
A person breathes an oxygen-deficient or toxic atmosphere, or flowing material surrounds them and restricts breathing or escape.	Tanks, silos, pits, vessels, trenches and other locations where hazardous atmospheres or engulfment can occur.
A fire, explosion or process release exposes a person to flame, heat, smoke, pressure, fragments or hazardous contents.	Hot work, hazardous-area work, chemical transfer, breaking containment, start-up, shutdown and abnormal process conditions.

Illustrative exposure pathway	Example work contexts
A structure or ground gives way, causing a person to fall or exposing them to falling or collapsing material.	Temporary works, excavations, stockpiles, demolition and work near unsupported structures.
A person falls into water or becomes submerged during work and cannot keep their airway clear or reach safety.	Work beside or over water, marine operations and diving activities.
A hazardous substance reaches a person through inhalation, skin or eye contact, or ingestion, in a single event or through repeated exposure.	Chemical manufacture, storage, transfer, use, spill response, maintenance and planned breaking of containment.
Respirable crystalline silica or other disease-causing dust becomes airborne and is inhaled during work, including through repeated or prolonged exposure.	Cutting, grinding, drilling, crushing, demolition, abrasive blasting and handling dusty materials.
Noise from plant, tools or high-impact activities reaches a person's ears at harmful levels, including through repeated or prolonged exposure.	Sustained or repeated exposure to hazardous noise from plant, equipment, tools or high-impact activities.

Appendix B: Illustrative critical controls for defined exposure pathways

These examples show how Section 6's four criteria can be applied to selected pathways in Appendix A. They are not prescribed solutions or technical specifications. Each control qualifies only where competent assessment and evidence demonstrate all four criteria for the actual exposure and conditions. Correct installation, use, maintenance and verification remain necessary; procedures and training support rather than replace the protection.

Read each example in order: direct action → protective capacity → protection when people make mistakes → objectively verifiable performance.

Exposure pathway and potential critical control	Conditions needed to meet all four criteria
Moving machinery **Exposure pathway:** A person or clothing reaches moving parts during normal operation. **Potential critical control:** fixed guarding that prevents access to the dangerous parts.	**1. Direct action:** physically prevents contact with moving parts. **2. Capacity:** strength, coverage and openings prevent serious-harm contact under the defined operating conditions. **3. Protection despite mistakes:** remains effective if someone reaches towards the danger zone or loses attention; it does not rely on a warning being followed. **4. Verifiability:** design evidence and competent checks confirm dimensions, fixings, condition and prevention of access. Visual presence alone does not prove capacity.

The guarding example covers normal operation, not access for cleaning, maintenance or fault-finding, which needs a separate assessment and effective protection.

Exposure pathway and potential critical control	Conditions needed to meet all four criteria
Hazardous energy during servicing **Exposure pathway:** Unexpected energisation or stored-energy release reaches a person working on equipment. **Potential critical control:** secured physical isolation, with stored energy safely removed or restrained.	**1. Direct action:** interrupts energy transmission or release into the work area. **2. Capacity:** addresses every relevant energy source and prevents harmful movement or release for the duration and conditions of the work. **3. Protection despite mistakes:** once correctly established, remains effective if someone attempts to operate a normal start control; protection does not depend on noticing a tag. **4. Verifiability:** competent checks establish effective isolation and control of stored energy using methods suited to the equipment. A permit or completed checklist alone is not proof.

Exposure pathway and potential critical control	Conditions needed to meet all four criteria
Disease-causing dust **Exposure pathway:** Dust escapes a process and is inhaled, including through repeated or prolonged exposure. **Potential critical control: an enclosed process with engineered extraction and automatic protection against loss of containment.**	**1. Direct action:** contains and removes dust before it reaches breathing zones. **2. Capacity:** competent assessment shows containment and extraction prevent serious illness from the defined substances, emission rates and exposure duration. Reduced dust or compliance with an exposure limit alone does not establish this. **3. Protection despite mistakes:** operation does not depend on a worker positioning a hood or responding to an alarm; automatic protection addresses foreseeable loss of containment or extraction before harmful exposure. **4. Verifiability:** commissioning and suitable containment, airflow, protective-function and exposure tests establish and confirm performance under representative operating conditions.

For dust, prove the required health protection rather than infer it from the presence of extraction. If evidence does not support the capacity or other criteria, do not designate the system as critical on this example alone. Other exposure routes, cleaning and maintenance need separate assessment. The implementation toolkits provide detailed assessment and verification methods.

Appendix C: Technical foundations and further guidance

This guide draws on established approaches to risk management, health and safety, critical control management, prevention of serious injuries and fatalities, governance and assurance. The resources below informed the principles and practices in the guide.

- ISO 31000:2018, Risk *management—Guidelines*, and ISO 45001:2018, Occupational *health* and *safety management systems—Requirements with guidance* for *use* (including Amendment 1:2024): risk management, leadership, participation and continual improvement.
- ICMM, *Critical Control Management: Good Practice Guide* (2026): current consolidated guidance on control selection, performance requirements, accountability, verification and response. The 2015 *Health and Safety Critical Control Management: Good Practice Guide* and *Critical Control Management: Implementation Guide* are earlier foundations, brought together in the 2026 edition.
- National Safety Council, *Serious Incident and Fatality (SIF) Prevention Model and Guidebook*: serious-harm potential, control effectiveness and learning before harm occurs.
- Energy-based and direct-control approaches: direct action on the hazard or exposure pathway, sufficient capacity to prevent serious harm from the defined exposure, protection when people make mistakes, forget something or lose attention during the work, and verification. This guide adapts these ideas into its four criteria; it does not adopt another model's definition in full.
- Institute of Directors and WorkSafe, Health and *Safety Governance: A Good Practice Guide* (2024): officer oversight, due diligence, assurance and evidence-based decisions.

The guide draws relevant principles from these sources and applies them in the New Zealand legislative context rather than adopting any one framework in full. Its approach is practical, led by operational management, supported by competent technical, specialist and H&S advice, and focused on the reliability and verification of critical controls, learning, escalation and governance oversight.

PCBUs should consult original resources for detailed technical or sector-specific methods. For the legal changes, use the Health and Safety at Work Amendment Act 2026 and WorkSafe's Understanding the changes to the health and safety law, including the PCBU-size and risk-management guidance signposted in Section 2. Check the applicable commencement dates and current versions before relying on them.

Restricted Content